
**מכרז למתן שירותי ניטור וניתוח
אירועי אבטחת מידע וסייבר עבור
חברת נתיבי איילון בע"מ**

מסמך ג' – מפרט השירותים

5	1	רקע על פעילות החברה
5	2	מערכות החברה
7	3	אתרי החברה
7	4	מטרות השירותים
8	5	תיחום השירותים
8	6	תנאים כלליים למתן השירותים
10	7	כללי
10	8	דרישות ממערכת ה SIEM
11	9	זכויות שימוש במערכת ה SIEM
12	10	תחזוקת מערכת ה SIEM
12	11	טיפול בתקלות במערכת ה SIEM
13	12	תמיכה טכנית
14	13	מטרות מוקד ה SOC
14	14	שיטת ההפעלה של מוקד ה SOC
15	15	צוות מוקד ה SOC
16	16	אמצעים לצוות המוקד
16	17	מערכות מוקד ה SOC
17	18	דרישות אבטחת מידע
17	19	פעולות שוטפות של מוקד ה SOC
18	20	שירותים מקצועיים נוספים – כללי
16	21	דוגמאות לשירותים נוספים
17	22	גיוס אנשי המקצוע נוספים
17	23	שינוי והחלפת אנשי מקצוע בצוות המקצועי
20	24	תקופת ההערכות - כללי
20	25	תכנון לתקופת ההיערכות
21	26	התאמת מערכת ה SIEM לשירותים הנדרשים
22	27	בדיקות מוכנות
23		נספח א' – פירוט מערכות בשימוש החברה
24		נספח ב' – נוסח כתב התחייבות לשמירת סודיות לצורך קבלת נספח א'

מונח	הגדרה
החברה/נתיבי איילון	חברת נתיבי איילון בע"מ.
הספק	מציע אשר יוכרו כזוכה במכרז עימו תחתום החברה על ההסכם ההתקשרות.
הסכם ההתקשרות/ההסכם	הסכם ההתקשרות אשר יחתם בין נתיבי איילון לבין מי שייבחר על ידיה כמציע הזוכה, אשר נוסחו מצורף כמסמך ב' למסמכי המכרז.
מערכות החברה	כלל המערכות הטכנולוגיות המשמשות את החברה.
ציוד קצה	חלק ממערכות החברה, הפרוס בשטח (כולל במשרדים, ובאתרי החברה) ומחובר למערכות החברה באמצעות רשת התקשרות.
האתר הראשי	האתרים בהם מותקנות ליבות מערכות החברה.
אתר DR	אתרים שישמש כגיבוי לאתר הראשי ויוקם במיקום שייקבע על ידי החברה.
אתר ה BCP	אתר המשמש כחלופה להפעלת מנת"ם דן במקרה חירום, הנמצא במשרדי החברה בעזריאלי ראשונים ראש"צ.
אתרי החברה	כלל האתרים הנמצאים באחריות החברה.
רשת התקשרות	רשת התקשרות הייעודית של החברה, המשמשת לחיבור ציוד קצה מסוגים שונים לליבת מערכות החברה, לרבות - התשתיות התת קרקעיות (צינורות ושוחות), רשת הסיבים האופטיים הפרוסים, מתגי התקשרות, מגשרי התקשרות, חיבורי החשמל וארונות התקשרות.
קבלני המערכת	כלל הקבלנים שנבחרו על ידי החברה לצורך הקמה ו/או הפעלה של מערכות החברה (לרבות זכיינים הפועלים במסגרת הסכמי זיכיון על פי הם החברה משמשת כרשות הממונה).
אירוע אבטחת מידע / סייבר	אירוע המשפיע או יכול להשפיע על פעילות החברה ו/או לגרום נזק למערכות החברה ו/או למידע האגור בהם.
המכרז	מכרז 84/24 למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ אשר פורסם על ידי החברה, על כל נספחיו, מסמכיו והעדכונים וההבהרות שיצורפו אליו.
מקור מידע	מערכת מידע / אפליקציה שהלוגים המופקים על ידה ו/או אירועים המתרחשים במסגרתה ייאספו אל המערכת.
מערכת ה SIEM	Security Information Event Management - מערכת לניטור, איסוף, וניתוח אוטומטי של נתונים ממערכות ותשתיות מידע, לגילוי וניהול אירועי אבטחת מידע המוצעת על ידי הספק במסגרת הצעתו למכרז והעומדת בכל הדרישות כמפורט במסמכי המכרז ובפרט במפרט זה.
לוג	רשומה המופקת ע"י ציוד או מערכת והכוללת מידע על אירוע שהתרחש באותו ציוד או מערכת.
חוק	תנאי לוגי המוגדר במערכת ה SIEM, שנועד לאתר קיום אירוע אבטחת מידע על בסיס מידע שדווח למערכת ה-SIEM.
אנליזה	סכימת התראות והצלבת אירועים על בסיס החוקים במערכת ה SIEM, למידע לאירוע אגרגטיבי, העשוי להצביע על קיום / חשש לקיום של אירוע אבטחת מידע.
התרעה	דיווח למשתמש בזמן אמת ובאמצעים שונים על קיום אירוע אבטחת מידע.
השירותים	השירותים נשוא המכרז, לרבות השירותים כמפורט בסעיף 1.5 לחוברת תנאי המכרז ובמפרט זה.
"מוקד SOC"	Security Operating Center - מוקד מאויש, שיופעל על ידי הספק ומטעמו בחצרי הספק, לצורך ניטור, אבחון ותגובה לאירועי סייבר ואבטחת מידע כמפורט במסמכי המכרז ובפרט במפרט זה.
צוות מוקד ה-SOC / צוות המוקד	צוות מטעם הספק המפעיל את מוקד ה-SOC ובכלל זה את מערכת ה-SIEM, ומטפל בהתרעות המתקבלות מהמערכת.
הצוות המקצועי	כלל הצוות שיועסק על ידי הספק לצורך מתן השירותים במסגרת ההסכם.
משרד התחבורה	משרד התחבורה והבטיחות בדרכים.

מכרז למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ

מונח	הגדרה
	ליתר המונחים המפורטים במסמך זה תהיה אותה המשמעות שהוגדרה להם בהסכם ההתקשרות, אלא אם צוין מפורשות אחרת.

להלן, קיצורים וראשי תיבות:

קיצור	פירוש
נת"י	נתיבי ישראל
DR	Disaster Recovery
GIS	Geographic Information System
GIV	מערכת ניהול התחזוקה של נת"א
SCADA	Supervisory Control And Data Acquisition
SOC	Security Operating Center
Sidera	מערכת ניהול ובקרת התנועה של החברה במנת"ם דן
SIEM	Security Information Event Management

פרק 1- סקירה על החברה ומערכותיה, מטרות השירות

בפרק זה יובא פירוט כללי על מערכות החברה, מטרות השירותים והגורמים המעורבים כרקע לשירותים.

1 רקע על פעילות החברה

- 1.1 נתיבי איילון משמשת כזרוע לביצוע מטלות של הממשלה באמצעות משרד התחבורה.
- 1.2 במסגרת זו ומבלי שהדבר יהווה מצג ו/או התחייבות של החברה, נכון למועד פרסום המכרז החברה מקימה ומפעילה מספר רב של פרויקטים בתחום התחבורה, ועיקרם:
 - 1.2.1 **הפעלת מרכזי ניהול התנועה (מנת"מים) במרחב דן ובמרחב המפרץ.** המנת"מים אחראים על ניהול התנועה במגוון רחב של צירי תנועה ועל ניהול מערכות הרמזור במספר ערים / יישובים.
 - 1.2.2 **פרויקט הזכיינות של הנתיבים המהירים** – פרויקט זכייני, במסגרתו יוקמו חניוני חנה וסע רבי קיבולת בשפיים ובראשלי"צ, ומהם יופעלו שירותי היסעים (שאטלים) ללב מטרופולין דן. שירותי ההיסעים אמורים לשמש כאלטרנטיבה לשימוש ברכב פרטי במרחב מטרופולין דן. הזכייין לפרויקט זה הינה חברת נתיב לעיר. החברה משמשת כרשות ממונה לפרויקט הזכייני.
 - 1.2.3 **פרויקט נתיבים מהירים ציר הרוחב** – פרויקט זכייני, במסגרתו יוקמו חניוני חנה וסע רבי קיבולת בצומת קסם ובצומת מורשה, ומהם יופעלו שירותי היסעים (שאטלים) ללב מטרופולין דן. שירותי ההיסעים אמורים לשמש כאלטרנטיבה לשימוש ברכב פרטי במרחב מטרופולין דן. הפרויקט נמצא בשלב המכרז. החברה משמשת כרשות ממונה לפרויקט הזכייני.
 - 1.2.4 **אופני דן** – הקמת והפעלת מערכת לניטור התנועה לאורך נתיבי האופניים בגוש דן (אופני דן).
 - 1.2.5 **פרויקט מס גודש** – פרויקט להקמת והפעלת תשתית למיסוי הגודש במרחב גוש דן. הפרויקט יכול כ-200 שערי אגרה. החברה משמשת כרשות הממונה להפעלת פרויקט זה.
 - 1.2.6 **פרויקט המתע"ן** – פרויקטים להקמת והפעלת תשתית לקווי הסעת המונים רבי קיבולת (BRT) באיזור לוד/ רמלה (הקו החום) ובאזור רחובות / נס ציונה / ראשלי"צ (הקו

- הכחול). הפרויקטים יכללו הקמת נתיב תחבורה יעודי לתנועת רכבי ה-BRT, וכן יטפל בממשקים בין תנועת ה-BRT לתנועת שאר הרכבים.
- 1.2.7 **פרויקט מהיר לעיר** – פרויקט להקמת נת"צים למתן עדיפות לנסיעת רכבי תחבורה ציבורית ורכבים בהם כמות מינימאלית של נוסעים.
- 1.2.8 **פרויקט אופני דן** – פרויקט להקמת והפעלת נתיבי תחבורה לאופניים ברחבי גוש דן.
- 1.2.9 **פרויקט המטרונית** – הפרויקט כולל מספר קווי BRT המופעלים באזור המפרץ. החברה אחראית לעבודות להרחבת הפרויקט, וכן להפעלת וניהול הפרויקט.
- 1.2.10 **פרויקט תשתית** להקמת נתיבי תחבורה בהם הרחבת כביש 20, כביש 200 ועוד.
- 1.2.11 פרויקטים לאיסוף, ניטור וניתוח מידע תחבורתי, לצורך תכנון ושיפור של תשתיות התחבורה בישראל.
- 1.3 קהל הלקוחות של החברה כולל את כל אזרחי ישראל. בנוסף, ומבלי שהדבר יהווה מצג ו/או התחייבות של החברה, נכון למועד פרסום המכרז החברה מספקת שירותים ייעודיים למספר גורמים נוספים:
- 1.3.1 **משרד התחבורה** - החברה משמשת כאמור כזרוע ביצוע של המשרד. בנוסף, החברה מספקת מידע תחבורתי המשמש לצורכי הפעלת מאגר נתוני העתק (Big Data) שהמשרד מפעיל לצרכי הציבור הרחב וכן לשימוש של גורמים המפעילים שירותים תחבורתיים (כגון – מפעילי קווי היסעים).
- 1.3.2 **משרד האוצר** – הפעלת פרויקטים זכיינים במסגרת שיתוף הפעולה עם המגזר הציבורי.
- 1.3.3 **רשויות מקומיות** - החברה משמשת כאמור כמנהלת התנועה של מערכות הרמזורים במספר רשויות, ונמצאת בתהליך קליטת ניהול התנועה כאמור ברשויות נוספות. בנוסף, החברה משמשת כזרוע הביצוע להקמה ושיפוץ של פרויקטים תחבורתיים בתחומי הרשויות השונות.
- 1.3.4 **גופי חירום וביטחון** – החברה מבצעת שיתוף פעולה במסגרת ניהול התנועה עם גורמי חירום וביטחון, לצורך ניהול אירועי חירום ומצבי קיצון הקשורים לניהול התנועה. ביניהם: משטרת ישראל, מד"א פיקוד העורף וכב"ה.
- 1.3.5 **חברות תשתית** – החברה פועלת בשיתוף פעולה עם חברות תשתית נוספות בפרויקטים משותפים / משיקים (בהם – נת"י, חוצה ישראל, נת"ע, רכבת ישראל וכו').
- 1.3.6 **קבלני מערכת** – ספקים המספקים שירותים לחברה, בקשר לתחזוקת ו/או הפעלת מערכות החברה, על בסיס הסכמים ביניהם לבין החברה.
- 1.3.7 **זכיינים** – גורמים המספקים שירותים מטעם החברה עבור מקטעים מסוימים (כגון הנתבים המהירים, מס הגודש וקווי המתע"ן).
- 1.3.8 **רשות ממונה** – גורם שימונה מטעם החברה לפקח על שירותי הזכיינים.

2 מערכות החברה

- 2.1 לצורך הקמת והפעלת הפרויקטים החברה נסמכת על מערכות טכנולוגיות רבות ומגוונות. מכרז למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ

גורמים המעוניינים רשאים לפנות לחברה בבקשה בכתב לכתובת דוא"ל orb@ayalohw.co.il לשם קבלת תיאור של המערכות המרכזיות הנמצאות בשימוש החברה נכון למועד פרסום המכרז (נספח א' למסמך זה). במסגרת הפניה כאמור נדרש לפרט את זהות הגורם המבקש ופרטי קשר למענה ולצרף כתב התחייבות לשמירת סודיות חתום בנוסח המצורף כנספח ב' למסמך זה. מובהר כי קבלת נספח א' כאמור הינה בכפוף לחתימה על כתב ההתחייבות כאמור להנחת דעתה של החברה וכי אין באמור כנספח א' כאמור כדי להוות מצג ו/או התחייבות של החברה.

2.2 מערכות החברה מוקמות ומופעלות על ידי קבלני מערכת הנבחרים על ידי החברה.

2.3 רשתות החברה: OT ו IT.

3 אתרי החברה

מבלי שהדבר יהווה מצג ו/או התחייבות של החברה, להלן תיאור נכון למועד פרסום המכרז -

3.1 החברה מפעילה 3 חדרי מחשב, בהם פועלות חלק מליבות המערכות הטכנולוגיות. יתרת המערכות הטכנולוגיות מופעלות כמערכות בענן / מערכות SaaS, ואשר הגישה אליהן הינה באמצעות תשתיות האינטרנט הארגוניות.

3.2 האתרים הראשיים מצאים בסבידור ולב המפרץ (רשת ה OT) ובראשון לציון (רשת ה IT).

3.3 באתר הראשי קיימת מרכזיה טלפונית IP המשרתת את כלל עובדי החברה. מרכזיה זו מושתת על 4 שרתים וירטואליים המתארחים על גבי שני שרתים פיזיים. בנוסף האתר הראשי מקבל שירותים מ 2 גורמים חיצוניים המחוברים בתשתיות IPVPN ואינטרנט.

3.4 האתר המשני מצוי בירושלים והינו העתק של המערכות והתשתיות של האתר הראשי (מנת"מ דן ומנת"מ המפרץ).

3.5 לחברה אתר BCP במשרדי החברה בראשל"צ.

4 מטרות השירותים

4.1 החברה מבקשת לקבל שירותים מגורם מתמחה, לצורך חיווי ובקרה של אירועי אבטחת מידע ומתן מענה בזמן אמת להפחתת אירועי הסייבר ולצורך טיפול יעיל ומהיר בהם, במטרה לאפשר רציפות תפקודית לפעילות החברה.

4.2 מטרות השירותים:

4.2.1 שיפור מוכנות החברה לאירועי אבטחת מידע וסייבר.

4.2.2 איסוף מידע ממגוון רחב ככל הניתן של מקורות, באמצעות מערכת ייעודית (SIEM), לגבי אפשרות לקיום אירועי אבטחת מידע או סייבר, שעלולים להשפיע על מערכות החברה.

4.2.3 מתן חיווי והתראות בזמן אמת לאירועים שעלולים להיות או זוהו כאירועי אבטחת מידע או סייבר, כשירות מנוהל מרחוק, באמצעות צוות מוקד ה- SOC כשירות Tier 1. האירועים יוגדרו על ידי החברה.

4.2.4 מתן שירותי אנליזה למידע המתקבל ממקורות המידע השונים, ביצוע ניתוח (אגרגציה, קורלציה ופורנזיקה) למידע המתקבל, כדי לגבש דרכי פעולה אפשריות להמשך הטיפול באירועים או מניעת קיומם כשירות ברמת Tier 2.

5 תיחום השירותים

- 5.1 הספק יידרש לספק שירות SOC כולל לחברה, על בסיס תשתית כללית שתופעל על ידי הספק, ולא כתשתית יעודית עבור החברה.
- 5.2 כעיקרון, על הספק לבצע את כל הנדרש לצורך ביצוע השירותים, ככל ולא נקבע מפורשות אחרת במפרט זה. האמצעים יכללו בין היתר (רשימה חלקית ולא ממצה):
- 5.2.1 אספקת זכויות שימוש במערכת SIEM – מערכת טכנולוגית לאיסוף המידע מהמקורות השונים, ניתוח המידע והפקת התרעות, בהתאם לדרישות בפרק 2 להלן. השירות יכלול מתן זכויות ורישוי למערכת ה SIEM כמפורט בהסכם ההתקשרות לרבות לצורך הגדרת חוקים בה וקישור שלה למערכות הרלוונטיות של החברה.
- 5.2.2 אספקת שירותי מוקד SOC – הפעלת מוקד לניתוח המידע והפקת התרעות, בהתאם למפורט בפרק 3 להלן. השירות יכלול את אספקת הצוות הנדרש ומיקום פיזי לפעילותו.
- 5.2.3 שירותים מקצועיים נוספים המפורטים בפרק 5 להלן.
- 5.3 למרות האמור לעיל, החברה תספק לספק את האמצעים הבאים:
- 5.3.1 שרתי Collector לצורך איסוף המידע ממערכות החברה והעברתן למערכת ה SIEM.

6 תנאים כלליים למתן השירותים

- 6.1 השירותים יסופקו עבור כל מערכות החברה ורשתות התקשורת שלה (כפי שיעודכנו מעת לעת על ידי חברה לפי שיקול דעתה הבלעדי לרבות כיום ואלה שיוקמו ויופעלו בעתיד).
- 6.2 השירותים יסופקו לחברה עצמה וכן לכל הגורמים המעורבים הקשורים לפעילות החברה (כגון – זכיינים הפועלים עבור החברה, קבלני משנה וכד').
- 6.3 השירותים יסופקו כ"שירות מנוהלי" על ידי הספק – הספק יידרש לספק את השירות מקצה לקצה, באופן מקצועי ובהתאם לכל הוראות מפרט השירותים וההסכם, כדי להבטיח את קיום מטרות השירותים.
- 6.4 השירותים יסופקו על בסיס מערכת ה SIEM, אשר הוצעה על ידי הספק במסגרת הצעתו למכרז, וכן על ידי צוות מקצועי יעודי אשר יועסק על ידי הספק לצורך ביצוע כלל השירותים, כפי שהנ"ל אושרו על ידי החברה, בהתאם לדרישות ההסכם.
- 6.5 החברה אינה מחויבת לרכוש שירותים מסוג או בהיקף מסוים. החברה תחליט בכל שלב במהלך תקופת ההתקשרות אילו שירותים לרכוש מהספק ואילו לא, בהתאם לשיקול דעתה.

- 6.6 כל הדרישות לשירותים המפורטות במפרט זה מהוות דרישות מינימום, ואין בהן כדי לפרט את כל הפעולות שעל הספק לבצע לצורך ביצוע השירותים. על הספק לבצע פעולות נוספות לצורך מתן השירותים, ככל והדבר יידרש, בהתאם ל-Best Practice.
- 6.7 פירוט השירותים במפרט מפורטים ברמה כללית בלבד. הספק נדרש להגיש לחברה פירוט מלא לכל אחד מהשירותים לאישורה במסגרת תקופת ההיערכות (כמפורט בפרק 5 להלן), וכן במהלך מתן השירותים השוטף כפי שיידרש על ידי החברה מעת לעת.
- 6.8 הצעת הספק כפי שאושרה על ידי החברה מהווה חלק בלתי נפרד מההסכם. ככל והספק יציע במסגרת המענה למכרז, הצעה המיטיבה יחסית למפורט במפרט זה – יהיה על הספק לספק את השירותים בהתאם להצעה העדיפה (לפי שיקול דעתה של החברה).
- 6.9 באחריות הספק לספק את השירותים, בהתאם לכל הדרישות וההוראות המחייבות החלות עליו (כל דין, תקנים, תקנות, חוקים, היתרים, הוראות המפרט הבין משרדי וכיוצ"ב).
- 6.10 על הספק להכיר וליישם את נוהל תגובה לאירוע סייבר של החברה כפי שיעודכן מעת לעת על ידי החברה.
- 6.11 הספק נדרש לקבל את כל האישורים, ההיתרים והרישיונות הנדרשים לביצוע כל השירותים, טרם תחילת ביצועם.
- 6.12 עבודה בחירום:
- 6.12.1 הספק יידרש להמשיך ולספק את השירותים גם בעת "מצב חירום".
- 6.12.2 לעניין זה - "מצב חירום" – במפרט זה: אירוע של פגעי טבע או אירוע הנובע ממצב לחימה שיש בו כדי לסכל, לשבש את השימוש בנתיבי התחבורה עליהם אחראית החברה או להפוך את השימוש בו למסוכן.
- 6.12.3 הצוות המקצועי מטעם הספק ירשם במרשם החברה לריתוק משקי והפעלה בחירום.
- 6.12.4 מבלי לגרוע מכלליות האמור לעיל על הספק להכיר וליישם את נוהל מס' 4.09 של החברה – "נוהל עבודה במצב חירום", בנוסחו העדכני, כפי שיעודכן מעת לעת.
- 6.12.5 קבעה החברה כי התרחש מצב חרום –
- 6.12.5.1 יתגבר הספק את הצוות המקצועי באנשי צוות נוספים לצורך טיפול וביצוע מטלות ההסכם ועמידה בהתחייבויות הספק על פיו.
- 6.12.5.2 יספק לאנשי הצוות המטפלים באירוע מטעמו, ציוד מתאים לצורך ביצוע מטלתם בכמות הנדרשת בהתאם למצב החירום.
- 6.12.5.3 יבצע כל פעולה נוספת באופן שיבטיח עבודה במשמרות רציפות מצד הצוות המקצועי.
- 6.12.6 למען הסר ספק, לא תשולם כל תוספת לספק, בגין פעולתו לפי סעיף זה.
- 6.12.7 יובהר כי אין בקיום אירוע חירום כדי לפגוע בשגרת הפעולות ולגרוע מהשירותים מהספק, בשינויים מחויבים.
- 6.13 מנגנון התמורה עבור השירותים מפורט בנספח ב' להסכם – התמורה. מכרז למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ

פרק 2 – מערכת ה SIEM – דרישות

בפרק זה יובא פירוט כללי הדרישות ממערכת ה SIEM שתסופק על ידי הספק כחלק מהשירותים.

7	כללי
7.1	הספק נדרש לספק מערכת SIEM, העונה על דרישות פרק זה, כחלק מהשירותים.
7.2	המערכת תהיה זו שהוצעה על ידי הספק במסגרת הצעתו למכרז, ואושרה על ידי החברה.
7.3	יובהר כי הדרישות המפורטות להלן הינן דרישות מינימום למערכת ה SIEM, וכי ככל והספק הציע יכולות העולות על הדרישות להלן – יידרש הספק לספק אותן כחלק ממערכת ה SIEM.
7.4	הספק יספק את כל הנדרש להקמת, תחזוקת והפעלת מערכת ה - SIEM.
8	דרישות ממערכת ה SIEM
8.1	המערכת תסופק כשירות Software as a Service - SaaS.
8.2	המערכת תעמוד בכל העומסים שיידרשו עבור החברה, ולפחות 3,000 אירועים לשנייה (EPS).
8.3	המערכת תקלוט התרעות ממקורות המידע שהוצעו על ידי הספק, ויכללו לפחות את מקורות המידע שיפורטו להלן:
8.3.1	מערך הסייבר הממשלתי.
8.3.2	מרכז הסייבר של משרד התחבורה.
8.4	המערכת תקלוט נתונים מכל סוגי מערכות ה OT ו ה IT של החברה שיפורטו להלן:
8.4.1	מערכת התחזוקה של החברה (מנת"א).
8.4.2	מערכות ה NOC של החברה.
8.4.3	מערכות הפעלה של שרתים ועמדות עבודה.
8.4.4	כלי אבטחת מידע אחרים בשימוש החברה.
8.4.5	ציוד תקשורת.
8.4.6	מערכות אחרות היוצרות SYSLOG.
8.5	המערכת תסנכרן את לוחות הזמנים השונים של מקורות המידע לשעון זמן אחוד.

- 8.6 מחזורי האיסוף (Collector) של המידע יוגדרו על ידי החברה, ויהיו נתונים לשינוי בהתאם להחלטת החברה באופן פשוט וללא תכנות. כמו כן תתאפשר קבלת מידע במשיכה.
- 8.7 המערכת תאפשר הגדרה של לפחות 5 רמות חומרה לאירועים (Severity Level). רמות החומרה ייקבעו על ידי החברה, ויהיו נתונים לשינוי בהתאם להחלטת החברה באופן פשוט וללא תכנות.
- 8.8 המערכת תאפשר הגדרת חוקים, אגרגציות, פרסור וקורלציות לכל אחת מהמערכות ומקורות המידע. המערכת תכיל סט חוקים בסיסיים (Out of the box).
- 8.9 המערכת תאפשר שליחת התרעות במגוון ערוצים – בהתאם להחלטת החברה – SMS, Whatsapp וכו'.
- 8.10 המערכת תשלב יכולות בינה מלאכותית (AI) לצורך לניתוח המידע וגיבוש תובנות.
- 8.11 המערכת תאפשר מעקב אחרי מחזור החיים של האירוע – ממועד קבלת המידע, מתן ההתרעה ודרך הטיפול. המערכת תאפשר הגדרת סטטוסים באופן גמיש, תוך קביעת סוג אירועים בהם מחוייב עדכון סטטוס וכאלה שלא.
- 8.12 המערכת תכלול כלי BI שיאפשר הצגת Dashboards לצורך תחקור האירועים והפקת תובנות רוחביות (סוגי האירועים, מקורות התקיפה, סוגי המערכות שהותקפו, ועוד).
- 8.13 המערכת תתעד את כל האירועים ותרשום לוג מפורט. הלוג יוכל להיות מיוצא למערכות אחרות ובפרט למערכת מנת"א.
- 8.14 המערכת תאפשר הפקת דוחות, תוך קביעת סוגי מיון וסינון גמישים על ידי משתמש הקצה. עיתוי משלוח הדוחות ורשימת התפוצה ייקבעו על ידי החברה.
- 8.15 המערכת תפעל ברציפות - 24 שעות ביממה 365 ימים בשנה.
- 8.16 המערכת תפעל באופן שמאפשר המשכיות עסקית ורציפות תפקודית.
- 8.17 המערכת תידרש לפעול בשרידות של 99.9% מהזמן בחישוב חודשי.
- 8.18 המערכת תנהל הרשאות בהתאם להחלטת החברה. כל משתמש יוכל לבצע תחקור בהתאם לרמת ההרשאה שתוקנה לו.
- 8.19 המערכת תכלול מערכת ניהול שתאפשר ניטור מלא של פעולתה בכל עת, ומשלוח התרעות על כל חריגה / תקלה.
- 8.20 המערכת תאפשר מעקב ביקורת על כלל פעילותה – שינויים בהרשאות, שינויים בהגדרות, שינויי גרסאות ולוגים.
- 8.21 המידע במערכת יישמר למשך 90 יום ב On line וב Off line לתקופה של שנתיים.

9 זכויות שימוש במערכת ה SIEM

- 9.1 הספק נדרש לספק את כל זכויות השימוש הנדרש למערכת, בהתאם להיקפי הפעילות שייקבעו על ידי החברה, כמפורט במפרט ובהסכם.

9.2 הרישוי יכסה את כל הדרישות ממערכת ה SIEM לפי הוראות פרק זה לרבות:

- 9.2.1 מענה לכל היכולות הנדרשות למערכת לפי הוראות ההסכם.
- 9.2.2 מענה לכל התכונות הנוספות שהוצעו על ידי הספק במסגרת הצעתו למכרז כפי שאושר על ידי החברה.
- 9.2.3 יכולות נוספות המוצעות על ידי היצרן ומוטמעות בגרסאות של המערכת המוצעות ללקוחות אחרים כפי שאושר על ידי החברה.
- 9.2.4 רישוי לכלי צד ג' המשולבים במערכת.
- 9.3 הספק יבצע עדכוני גרסאות למערכת בהתאם להוראות היצרן. כמו כן, הספק יבצע עדכוני גרסאות במועדים הבאים:
 - 9.3.1 אירועי אבטחת מידע.
 - 9.3.2 עדכון בחוקת המערכת.
 - 9.3.3 בעת גילוי באג במערכת.
 - 9.3.4 עדכונים בסביבת הענן בה מותקנת המערכת.
- 9.4 בכל מקרה לא יעלה מועד העדכון על 30 ימי עבודה ממועד היווצרות הסיבה לעדכון.

10 תחזוקת מערכת ה SIEM

- 10.1 הספק נדרש לספק שירותי תחזוקה למערכת ה SIEM.
- 10.2 תקופת ההפעלה והתחזוקה תחל עם קבלת האישור להפעלת השירות כמפורט בסעיף 27.4 להלן.
- 10.3 במהלך תקופת התחזוקה תחול על הספק אחריות בלעדית לתחזוקת המערכת, לרבות תיקון כל ליקוי שיתגלה בהם.
- 10.4 הספק יספק את שירותי התחזוקה באופן שיביא לעמידה מלאה בכל רמות השירות המפורטות במפרט זה ("רמות השירות").
- 10.5 הספק יוודא כי פעולות התחזוקה יבוצעו בהתאם להוראות היצרן, באופן שלא יביא להפרת האחריות של הספק או להפרת תנאי זכויות השימוש.
- 10.6 שירותי התחזוקה יבוצעו על ידי הספק באמצעות גורמים מורשים מטעם היצרן אשר יידרשו לאישור פרטני ובכתב על ידי החברה.

11 טיפול בתקלות במערכת ה SIEM

- 11.1 הספק מחויב להתחיל בביצוע תיקון התקלות בהתאם לרמות השירות שיפורטו להלן.
- 11.2 הספק נדרש להודיע לפחות 7 ימי עבודה לפני השבתה מתוכננת.
- 11.3 זמני תחילת הטיפול בתקלות יהיה על פי דרגות החומרה, בהתאם למפורט בטבלה הבאה:

דרגת חומרה	סוג תקלה	זמן תחילת טיפול מקסימאלי
1	תקלה קריטית – תקלה הגורמת להשבתה כללית של המערכת או חוסר זמינות של מקורות המידע	עד 4 שעות, הטיפול יימשך באופן רציף במהלך כל שעות היממה (24 שעות), ובמשך 365 ימים בשנה.

מכרז למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ

2	תקלה דחופה – תקלה הפוגעת בצורה משמעותית בפעילות המערכת	עד 4 שעות, הטיפול יימשך באופן רציף במהלך השעות 8-17 בימים א'-ה' ובין השעות 8-12 בימי ו'.
3	תקלה רגילה – תקלה שאינה קריטית ואינה דחופה.	עד תום יום העסקים העוקב. הטיפול יימשך באופן רציף במהלך השעות 8-17 בימים א'-ה' ובין השעות 8-12 בימי ו'.

- 11.4 ההגדרה אם מדובר בתקלה וכן רמת הסיווג של התקלות ייקבעו על ידי החברה.
- 11.5 במקרה של תקלה קריטית או דחופה - על הספק לפעול לתיקון התקלות עד השלמת תיקון התקלה, או עד השלמת ביצוע מעקף המאפשר עבודה תקינה. מגמר השלמת המעקף ואישורו, ירד סיווג התקלה ל"רגילה".
- 11.6 הספק נדרש לבדוק את תיקון התקלה בסביבת ה Test לפני העלאת הגרסה לסביבת הייצור.
- 11.7 הספק נדרש לתעד את כל התקלות. הספק יעביר לחברה דו"חות חודשיים על תקלות.

12 תמיכה טכנית

- 12.1 הספק יידרש לספק תמיכה טכנית (Help desk) למערכת.
- 12.2 מנגנון התמיכה הטכנית שיסופק על ידי הספק יסייע לנציגי החברה בכל נושא הקשור להפעלת המערכת (לרבות בנושאי מוצרי צד ג' ששולבו בה):
- 12.2.1 סיוע והדרכה שוטפת להפעלה.
- 12.2.2 סיוע בבעיות ותקלות.
- 12.3 התמיכה מטעם הספק תספק מענה אנושי על ידי אנשי מקצוע במהלך 24 שעות ביממה, 365 ימים בשנה.
- 12.4 זמני תגובה נדרשים לשירותי התמיכה הטכנית:
- 12.4.1 לכל פנייה תימסר הודעה אוטומטית המאשרת את מועד קבלת הפנייה ומעדכנת את הפונה על משך הטיפול הצפוי.
- 12.4.2 זמן תגובה למענה על ידי גורם מקצועי מטעם הספק (שהינו אדם בעל יכולת טכנית לטיפול בתקלות מורכבות) בתקלה קריטית או דחופה לא יעלה על 20 דקות, ו 60 דקות לפניות אחרות, הכל מרגע קבלת הפנייה.
- 12.4.3 במקרה הצורך תבוצע אסקלציה על ידי הפניית קריאות למרכזי התמיכה של היצרן. על הספק להעביר את הפנייה לנציגות היצרן תוך 24 שעות מרגע קבלתה, ככל ולא החל בטיפול בה.
- 12.5 על הספק יהיה לנהל את כל הקריאות שיופנו לתמיכה הטכנית (כולל תיעוד של מהות הפנייה, סטטוס הטיפול, לוחות הזמנים לטיפול והמענה שניתן) באמצעות מערכת יעודית שתסופק על ידו.
- 12.6 בסוף כל חודש יונפק לחברה דו"ח פניות הכולל את פרטי הפניות. תכולת הדו"ח תוגדר על ידי החברה.

פרק 3 – מוקד ה SOC

בפרק זה יובא פירוט להפעלת מוקד ה SOC.

13 מטרת מוקד ה SOC:

13.1 הספק נדרש להפעיל מוקד SOC לצורך שיפור יכולות הזיהוי והניתוח של אירועי אבטחת מידע, ושיפור דרכי ההתמודדות עם אירועים אלה.

13.2 מוקד ה SOC יפעל על בסיס מידע שיסופק על ידי מערכת ה SIEM. במוקד ה SOC יבוצע עיבוד ברמות שונות למידע המתקבל ויעברו התרעות בזמן אמת למערכות החברה ולגורמים מטעמה.

14 שיטת ההפעלה של מוקד ה SOC

14.1 מוקד ה SOC יפעל כשירות מנוהל ממקום מרוחק, בשטח מדינת ישראל.

14.2 מוקד ה SOC יופעל באופן רצוף 24 שעות ביממה, 365 ימים בשנה. המוקד יופעל על בסיס משמרות מתחלפות של צוות מוקד ה- SOC המקצועי מטעם הספק.

14.3 מוקד ה SOC יפעל ב 2 רמות עבודה:

14.3.1 Tier 1 – ניתוח ראשוני של המידע המועבר ממערכת ה SIEM, סיווג האירוע, העברת דיווח ראשוני והחלטה על המשך הטיפול (סגירה או העברה ל TIER 2).

14.3.2 Tier 2 – ביצוע ניתוח מעמיק של האירוע (כולל קורלציות ואגרזציות בין מספר אירועים נפרדים), זיהוי מערכות בסיכון, המלצה על התגובה, פעולות למניעת התפשטות, תיקון וחזרה לשגרה ותמיכה בצוות ה IR מטעם החברה (ככל ויפרס).

14.4 מוקד ה SOC יופעל על ידי צוות מוקד ה- SOC המקצועי, שיעמוד בדרישות שיפורטו להלן. בכל משמרת יכלול הצוות לפחות את בעלי התפקיד (העומדים בדרישות המפורטות בסעיף 15 להלן) להלן:

14.4.1 מנהל משמרת.

14.4.2 לפחות 2 בקרים לטיפול ברמת Tier 1.

14.4.3 לפחות אנליסט אחד לטיפול ברמת Tier 2.

14.5 המוקד יסווג את האירועים בלפחות 3 רמות חומרה (רמות החומרה יוגדרו בתקופת ההיערכות כמפורט בפרק 5 להלן).

14.6 המוקד יקבל מידע ממערכות החברה ויתריע בהתאם לחומרת האירועים כאמור. מוקד ה- SOC יתריע על כל הפעולות הבאות לפחות:

14.6.1 כשלים ועומסים שדווחו ממוקד ה NOC של החברה.

14.6.2 זיהוי אובייקטים (משתמשים וקבוצות) חדשים.

14.6.3 פעילות של משתמשים חסומים ושל משתמשים שבוטלו.

מכרז למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ

- 14.6.4 יצירה/הוספת/שינויים בהרשאות.
- 14.6.5 התחברות עם כלים לא מורשים (כגון אמצעים נתיקים) ליחידות הקצה
- 14.6.6 כשלים בהזדהות למערכות.
- 14.6.7 יצירת משתמשים בתחנות העבודה.
- 14.6.8 כניסות למאגרי מידע שיוגדרו כרגישים.
- 14.6.9 הודעה על אי זמינות של יחידת OT.
- 14.6.10 מחיקת קבצים או הודעות דוא"ל מאסיבית.
- 14.7 תובטח ההמשכיות התפקודית של מוקד ה SOC - בין היתר באמצעות אתר חלופי (אתר DR) אשר נבדק ותורגל, המאפשר המשך פעילות של המוקד, בעת פגיעה באתר הראשי, או בשעת חירום וזאת בתוך שעתיים מהשבתת האתר הראשי.

15 צוות מוקד ה SOC

- 15.1 הספק יספק אנשי מקצוע למוקד ה SOC שיעמדו בדרישות המינימליות המפורטות להלן:

תפקיד	דרישות מינימום	הכשרה / השכלה
מנהל חדר הבקרה	בעל ניסיון של 3 שנים בניהול מוקד SOC שבו הועסקו לפחות 3 בקרים ואנליסטים, ואשר קיבל מידע בהיקף של לפחות EPM 2,500.	
אנליסט	ניסיון של שנתיים לפחות בהכנת ועדכון חוקים במערכת ה SIEM המוצעת.	בעל הסמכה של CCNA או CCNP בעל הסמכה של Cyber Security Analyst או Certified incident Handler או ethical Certified Hacker.
בקר	ניסיון של 6 חודשים כבקר במוקד SOC של ארגון גדול. ניסיון בהפעלת מערכת ה SIEM המוצעת ובעדכון חוקים בה.	

- 15.2 על הספק לאייש את צוות המוקד בהתאם לדרישות האיוש המינימליות כאמור בסעיף 14 לעיל וסעיף 15 זה לצורך עמידה בהיקפי האיוש הנדרשים בכל משמרת. לפיכך, באחריות הספק לאייש את הצוות במוקד בכמות כח האדם שתאפשר עמידה בדרישה זו, תוך התחשבות בכל הנסיבות האפשריות בגינן צפויה היעדרות של מי מאנשי צוות המוקד (לרבות בשל תחלופה, מחלה, חופשים ועוד).
- 15.3 כל בעל תפקיד יוכל למלא תפקיד אחד בלבד. הספק לא יוכל לאייש 2 תפקידים או יותר על ידי אדם אחד.
- 15.4 יובהר כי אין בפירוט הדרישות לגבי צוות המוקד כדי למצות את כלל אנשי הצוות והמשאבים האחרים שיידרשו מאת לספק לשם מתן השירותים, וכי זו אחריותו הבלעדית של הספק לספק את כלל אנשי הצוות, המשאבים והאמצעים הנדרשים כדי לעמוד בדרישות השירות שהוגדרו במפרט זה, גם אם לא צוינו במפורש.

- 16.1 הספק נדרש לספק לצוות המוקד את כלל האמצעים הנדרשים לצורך מתן השירותים, ולקבל את אישור החברה עבורם מראש.
- 16.2 הציווד והאמצעים לצוות המקצועי יכלול:
- 16.2.1 אספקת ציוד מחשוב.
 - 16.2.2 אמצעים פריפריאליים (סורקים ומדפסות).
 - 16.2.3 ציוד מתכלה (כגון - דפים, ציוד משרדי וסוללות).
 - 16.2.4 רישוי הנדרש לביצוע השירותים (כולל מערכות הפעלה, כלי Desktop, כלי אבטחת מידע ותוכנות שיתוף מידע).
 - 16.2.5 אמצעי תקשורת (טלפונים ניידים ואמצעים לקיום דיונים מרחוק).
 - 16.2.6 קווי הקישור ותעבורת הנתונים באמצעות רשת טלפונית או רשת האינטרנט.
 - 16.2.7 אמצעי תחבורה ו/או שירותי חנייה.
 - 16.2.8 הוצאות אש"ל ומזון.
- 16.3 הספק נדרש לוודא כי כלל הציוד, המשאבים והאמצעים שיועמד לרשות הצוות מטעמו יהיה תקין בכל עת, וזמין בהתאם להיקף השירותים ולסוג השירותים
- 16.4 הספק נדרש לוודא כי כל הצוות מטעמו פועל בהתאם להנחיות הבטיחות המקובלים ולהנחיות הבטיחות של נתיבי איילון. הספק נדרש לעבוד בהתאם להוראות ובתיאום עם אחראי הבטיחות מטעם החברה.
- 16.5 הספק יידרש לספק לצורך כך את כל האמצעים הנדרשים לחיבור מרחוק למערכות החברה (חומרה, אמצעי קצה, מחשב/מסוף, תוכנות והרישוי הנדרש), בהתאם לתצורת החיבור שתיקבע מעת לעת ע"י החברה.

17 **מערכות מוקד ה SOC**

- 17.1 המוקד יהיה מצויד במערכות הבאות לפחות:
- 17.1.1 מערכת ה SIEM.
 - 17.1.2 מערכת שו"ב לבדיקת קבלת המידע ממקורות המידע השונים.
 - 17.1.3 מערכת לניהול ותיעוד הטיפול בהתראות ובאירועים ticketing.
 - 17.1.4 מערכת (SOAR (security orchestration, automation and response) אשר מאפשרת לייצר ולקבוע תהליכי תגובה והכלה אוטומטיים בהתאם למתודולוגיית ומדיניות החברה.
 - 17.1.5 מערכת בקרת כניסה המאפשרת כניסה על בסיס 2FA.
 - 17.1.6 מערכת אבטחה הכוללת מרכזת, מצלמות אבטחה וחיישנים.
- 17.2 מוקד ה SOC יחובר לתשתיות תקשורת ומתח מתקדמות, ללא נקודת כשל יחידה (single point of failure), עם גיבוי ויתירות מלאים, שיאפשרו המשכיות תפקודית.

17.3 כלל מערכות המוקד יוצגו לאישור החברה במהלך תקופת ההערכות כהגדרתה בהסכם ההתקשרות (לרבות כמפורט בפרק 5 להלן).

18 דרישות אבטחת מידע

18.1 עמידה בדרישות כמפורט במסמך דרישות אבטחת המידע המצורף כמסמך ד' למסמכי המכרז.

19 פעולות שוטפות של מוקד ה SOC

19.1 מוקד ה SOC יופעל בהתאם להוראות החברה.

19.2 שירותי הפעלת מוקד ה SOC יכללו:

19.2.1 עדכון חוקים במערכת ה SIEM על בסיס לקחים.

19.2.2 עדכון תרחישי ההפעלה (Play book).

19.2.3 חקירות פורנזיות ראשוניות של האירועים.

19.2.4 תיאום מקורות המידע למול מוקדי SOC מקבילים.

19.2.5 הדרכה שוטפת לגורמי החברה בנושא הימנעות מאירועי סייבר.

19.2.6 השתתפות בלפחות 2 תרגילים בשנה לבחינת מוכנות החברה לאירועי סייבר ביוזמת החברה.

19.2.7 הפעלת צוות ה IR מטעם החברה, בהתאם לצורך.

19.3 מוקד ה - SOC יפעל בהתאם לרמות השירות המינימאליות לתגובה להלן (בדקות מההתרעה ב SIEM ועד לתחילת טיפול):

רמת קריטיות	קריטיות	גבוהה	רגילה
הבחנה בהתראה ותחילת טיפול Tier1	2	10	30
דוח ועדכון מערכת Ticketing \ Soar	4	15	45
סיום הטיפול והחלטה ברמת Tier1 (סגירה או העברה ל Tier 2)	7	30	60
תחילת ניתוח ע"י Tier2	7	15	60
דיווח לחברה	15	30	90

19.4 בכל מקרה של אי עמידה ברמות השירות – הספק יחויב בפיצויים מוסכמים כמפורט בהסכם.

פרק 4 – שירותים מקצועיים נוספים

20 שירותים מקצועיים נוספים – כללי

- 20.1 החברה תוכל לבקש מהספק שירותים מקצועיים נוספים כדוגמת המפורטים בסעיף 21 להלן, הקשורים להפעלת וניהול מערכות אבטחת המידע המופעלות על ידה.
- 20.2 השירותים יסופקו על בסיס שעות עבודה בהתאם לצורך ולהזמנת החברה בכתב כמפורט בהסכם ההתקשרות.
- 20.3 השירותים יבוצעו על ידי צוות מקצועי רלוונטי. הדרישות ייקבעו על ידי החברה בהתאם למהות השירותים. לצורך השירותים, בהתאם להוראות לכך בסעיף 22 להלן.
- 20.4 כלל השירותים המקצועיים הנוספים בפרק זה יבוצעו (ככל שיוזמנו על ידי נתיבי איילון) תחת הנחייתה ופיקוחה של ראשת תחום אמו"ס בנתיבי איילון ו/או מי מטעמה.
- 20.5 יובהר כי החברה לא מחויבת לרכוש שירותים מסוג או בהיקף מסויים, ולספק לא תהיה כל טענה ו/או דרישה ו/או תביעה בנושא.

21 דוגמאות לשירותים נוספים

- מבלי שהדבר יהווה מצג ו/או התחייבות של החברה, להלן דוגמאות לשירותים נוספים שנתבי איילון רשאית להזמין מידי הספק:
- 21.1 כתיבת או עדכון של נהלי אבטחת מידע והדרכות, כדוגמת הבאים:
- 21.2 כתיבת מסמכי מדיניות.
- 21.3 הכנת ועדכון נהלי אבטחת מידע.
- 21.4 הכנת לומדות ועזרי הדרכה להדרכות.
- 21.5 מתן הדרכות לעובדי החברה בתחום אבטח המידע.
- 21.6 עריכת שאלונים ומבחני הסמכה.
- 21.7 סקרים לעמידה בתקנים מחייבים (GDPR, 27001 וכד).
- 21.8 נוהל מפורט (Play Book) לפעולה בעת אירוע סייבר.

22 גיוס אנשי המקצוע נוספים

- 22.1 החברה תגדיר דרישות מקצועיות ביחס לשירותים המקצועיים הנוספים יוזמנו על ידה.
- 22.2 הספק נדרש להציג לאישור החברה עבור כל מטלה, לפני ביצועה בפועל.

22.3 עבור בעלי תפקיד מסוימים (מומחה אבטחת מידע וסייבר ומומחה פרטיות), נדרש הספק להציג מועמדים במהלך תקופת ההערכות כמפורט בפרק 5 להלן. שאר אנשי המקצוע יוצגו לפי הצורך ולדרישת נתיבי איילון.

22.4 הספק מתחייב להמציא לידי החברה את כל המסמכים הנדרשים לצורך הוכחת עמידת אנשי הצוות המקצועי בדרישות הרלוונטיות.

22.5 אנשי המקצוע יוצגו לאישור החברה תוך 30 ימי עבודה ממועד קבלת הבקשה.

22.6 המועמדים ירואיינו וייבחנו ויאושרו על ידי נציג החברה. החברה תוכל לסרב להצבתם של מועמדים מסוימים המוצעים על ידי הספק.

22.7 הספק יידרש להציב את אנשי המקצוע שיאושרו על ידי החברה בתפקידם תוך עד 14 ימי עבודה לאחר קבלת אישור החברה.

22.8 כל חברי הצוות המקצועי שיאושרו על ידי החברה, יהיו זמינים למתן שירותים לחברה בתוך 48 שעות מהזמנת השירות על ידי החברה, במהלך שעות העבודה הרגילות.

23 שינוי והחלפת אנשי מקצוע בצוות המקצועי:

23.1 החברה תוכל לדרוש מהספק כי יחליף אחד או יותר מבעלי המקצוע הנכללים בצוות המקצועי בכל עת ומכל סיבה סבירה, והספק ימנה איש מקצוע חלופי תוך עד 20 ימי עבודה.

23.2 במקרה שחבר בצוות המקצועי יחליט על סיום עבודתו אצל הספק - יודיע הספק על כך לחברה מיד עם היוודע לו הדבר.

23.3 הספק יתחייב לכך שהחלפת נציג בצוות המקצועי מכל סיבה שהיא לא תפגע בהתחייבויותיו על-פי מכרז זה.

23.4 החלפת חבר בצוות המקצועי תאושר רק לאחר מינוי מחליף. המחליף יהיה בעל כישורים שאינם נופלים מחבר הצוות המקצועי המוחלף, בהתאם לשיקול דעתו של נציג החברה.

פרק 5 – תקופת ההערכות

24 תקופת ההיערכות - כללי

- 24.1 הספק נדרש להקים את מוקד ה SOC במהלך תקופת ההערכות כהגדרתה בהסכם ההתקשרות ותוך עד 60 ימי עבודה ממועד חתימת הסכם ההתקשרות (במקביל להקמת מערכת ה SIEM).
- 24.2 מבלי לגרוע מהאמור מובהר כי הספק עשוי להידרש להעסיק בעלי תפקידים מסוימים לצורך מתן השירותים המקצועיים הנוספים, כמפורט בפרק 5 לעיל.

25 תכנון לתקופת ההיערכות

- 25.1 הספק נדרש להגיש תוכנית עבודה להקמת מוקד ה SOC תוך עד 7 ימי עבודה מתחילת תקופת ההיערכות. התוכנית תכלול התיחסות לנושאים הבאים:
- 25.1.1 מיקום פיזי של המוקד.
 - 25.1.2 הצגת מערכות המוקד.
 - 25.1.3 תוכנית לגיוס השמה והדרכה של צוות המוקד.
 - 25.1.4 תוכנית פעולה ונהלים להפעלת מוקד ה SOC .
 - 25.1.5 תרחישי פעולה (Playbook) למגוון סיכונים.
 - 25.1.6 הגדרת מקורות המידע.
 - 25.1.7 הגדרת סוגי אירועים ורמות חומרה, בהתאם למפורט בסעיף 19 לעיל
 - 25.1.7.1 רמה קריטית – השבתה או חשש להשבתה של מערכת ממערכות החברה באופן מלא או באופן משמעותי.
 - 25.1.7.2 רמה גבוהה – השבתה או חשש להשבתה של פעילות משמעותי במערכת החברה, הגורמת לירידה משמעותית בפעולתה.
 - 25.1.7.3 רמה רגילה – כל אירוע אחר.
 - 25.1.8 הגדרת סוגי הדיווחים שיועברו ורשימות התפוצה.
 - 25.1.9 שגרת הפעלת מוקד ה SOC - הגדרת משמרות, הגדרת כמות צוות המוקד כדי לספק שירות, הדרכות יומיות, בקרה וריענון.
 - 25.1.10 היערכות לשמירה על שרידות והמשכיות עסקית.
 - 25.1.11 לוח זמנים מפורט להשלמת תקופת ההיערכות.
- מכרז למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ

- 25.1.12 תוכנית לבדיקת מוכנות הספק להפעלת מוקד ה - SOC (כולל מוכנות של מערכת ה SIEM).
- 25.1.13 מענה לדרישות אבטחת מידע.
- 25.1.14 פירוט דוחות ודיווחים.
- 25.2 החברה תוכל להעיר על התוכנית, והספק יידרש לתקן את התוכנית בהתאם.
- 25.3 לאחר אישור החברה יידרש הספק לבצע את המפורט בתוכנית המאושרת במהלך תקופת ההערכות.
- 25.4 תהליך ההקמה יובל על ידי מנהל פרויקט יעודי מטעם הספק, בעל ניסיון בהקמת מוקד SOC בהיקף דומה.
- 25.5 במהלך תקופת ההיערכות ייערכו דיוני סטטוס מדי שבוע אצל החברה, במטרה לוודא את התקדמות תהליך ההיערכות.
- 26 התאמת מערכת ה SIEM לשירותים הנדרשים**
- 26.1 במסגרת תקופת ההערכות, הספק נדרש לבצע התאמה של מערכת ה SIEM לשירותים הנדרשים.
- 26.2 במסגרת ההתאמות הספק נדרש לבצע את הפעולות הבאות:
- 26.2.1 מיפוי תכנון מפורט וביצוע של לקישור הנדרש לצורך העברת המידע למערכות החברה (Collector) והקמת הקישור בין המערכת לבין מערכות החברה. הקישור יאובטח באמצעות FW ב 2 קצותיו.
- 26.2.2 הגדרת ממשק המשתמש למערכת, לרבות – UI / UX עיצוב מסכים, דשבורדים (Dashboards) ופורטל Admin.
- 26.2.3 הגדרת מערכת הניהול – מתן הרשאות, שמירת לוגים וניטור היקפי פעילות.
- 26.2.4 ממשקים למערכת השו"ב של החברה.
- 26.2.5 הצגת עקרונות לפיתוח החוקה למערכת, כולל הסבת חוקים קיימים והגדרת חוקים חדשים.
- 26.2.6 אפיון דוחות המערכת (כולל מיונים, סיווגים, Dashboards, עיתוי הפקה ולוחות תפוצה).
- 26.2.7 הגדרת בדיקות קבלה נדרשות. יוגדרו – סוגי הבדיקות, תסריטי בדיקה, תנאים להצלחת הבדיקות, מועדים צפויים לעריכת הבדיקות.
- 26.2.8 פירוט תכולת התיעוד של המערכת.
- 26.2.9 לוח זמנים מפורט להקמת המערכת (בהתאם ללוח הזמנים המקסימלי שפורט לעיל).
- 27 בדיקות מוכנות**
- 27.1 בתום תהליך ההיערכות יבצע הספק בדיקות מוכנות למוקד ה SOC ושימוש במערכת ה SIEM.

27.2 במהלך בדיקות המוכנות יבוצעו תרחישים בהתאם לתוכנית שאושרה מראש ובכתב על ידי החברה במהלך תקופת ההערכות.

27.3 על הספק לכלול בבדיקות המוכנות בין היתר את הבדיקות הבאות:

27.3.1 בדיקת עומסים.

27.3.2 ביצוע בדיקות חדירה (PT).

27.3.3 הפעלת מערכת ההרשאות.

27.3.4 קבלת המידע ממקורות המידע.

27.3.5 הפעלת כלל הממשקים למערכות החברה.

27.3.6 הרצת חוקים במערכת ה-SIEM (כול להסבת החוקים הקיימים).

27.3.7 בדיקת מוכנות היישום להפעלה ותחזוקה.

27.4 הבדיקות יבוצעו על ידי הספק. החברה תוכל לדרוש להיות נוכחת במהלך הבדיקות, לפי שיקול דעתה.

27.5 ככל ויתגלו תקלות בהפעלת מוקד ה-SOC במהלך בדיקות המוכנות – הספק יידרש לתקן, והכל במסגרת לוח הזמנים שהוגדר לתקופת ההיערכות.

27.6 הספק יידרש לספק לחברה את תוצאות הבדיקות באופן מלא, כולל תיקון ליקויים שהתגלו במהלך.

27.7 בתום בדיקות המוכנות, ולאחר תיקון הליקויים, יידרש הספק לבקש מהחברה אישור הפעלה למוקד ה-SOC (האישור להפעלת השירות כהגדרתו בהסכם ההתקשרות). מתן האישור כאמור יותנה בהשלמת כל המטלות מהספק לצורך הקמת מוקד ה-SOC והפעלת מערכת ה-SIEM, הכל בהתאם להסכם ההתקשרות.

נספח א' – פירוט מערכות בשימוש החברה נכון למועד פרסום המכרז

לעניין זה ראו סעיף 2.1 למפרט השירותים

נספח ב' – נוסח כתב התחייבות לשמירת סודיות לצורך קבלת נספח א'

תאריך: _____

לכבוד
חברת נתיבי איילון בע"מ
משד' נים 2 עזריאלי ראשונים
ראשל"צ 7546302

ג.א.ג.

הנדון: התחייבות לשמירת סודיות

אני/הח"מ, _____, ת.ז.ח.פ.ע.מ. _____, מצהיר/ים בזאת כלפי חברת נתיבי איילון בע"מ (להלן: "**נתיבי איילון**"), כי ידוע לי/לנו שנתיבי איילון עשויה להעביר לי/לנו את נספח א' למפרט השירותים מבלי שהדבר יהווה מצג ו/או התחייבות מצידה ולצורך הערכות להגשת הצעה במסגרת מכרז 84/24 למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ (להלן: "**המכרז**") ו-**נספח א'**, בהתאמה) בלבד וכי במסגרת נספח א' ייחשף בפנינו מידע של נתיבי איילון אשר הינו נכס מנכסיהם העיקריים והחיוניים ביותר של נתיבי איילון, לפי העניין.

בכתב התחייבות זה, המונח "**מידע**" משמעו, כל מידע וכל נתון המפורט בנספח א', ולמעט מידע שהינו נגיש ופתוח לעיון הציבור.

לפיכך אני/ מצהיר/ים ומתחייב/ים כלפי נתיבי איילון כדלקמן:

1. לשמור בסודיות מוחלטת את המידע ולא לגלותו ו/או להעבירו, במישרין או בעקיפין, לכל אדם ו/או גוף כלשהו, לרבות עובדי נתיבי איילון, שהמידע אינו נחוץ להם לצורך מילוי תפקידם והכל לשם הגשת הצעת/נו במסגרת המכרז.
2. לא למסור ו/או להעביר, במישרין או בעקיפין, לכל אדם ו/או גוף כלשהו, חומר, מסמך, דיסקט, דיסק, החסן נייד ו/או כל כלי אחסון אחר, המאחסן את המידע, ולא לעשות, במישרין או בעקיפין, כל שימוש במידע, כולו או מקצתו, לרבות שכפול, ייצור, מכירה, העברה, הפצה, שינוי, העתקה ו/או חיקוי, למעט כאמור בסעיף 1 לעיל, בהסכמת נתיבי איילון, ולטובתה בלבד.
3. למסור לנתיבי איילון, את המידע וכל כלי אחסון אחר המכיל את המידע לרבות כאמור בסעיף 2 לעיל, שיימצא ברשותי/נו ו/או בשליטתי/נו, מייד עם דרישתה הראשונה של נתיבי איילון ובכל מקרה לא יאוחר מחלוף המועד האחרון להגשת הצעות למכרז.
4. אני/נו מודע/ים לכך שהפרת התחייבויותיי/נו על פי כתב התחייבות זה, או חלק מהן, עלולה לגרום לנתיבי איילון ו/או לגופים הקשורים בה, נזקים חמורים ביותר ובלתי הפיכים אשר פיצוי כספי לא יהווה תרופה וסעד נאות להם, ולפיכך אני/נו מסכים כי נתיבי איילון תהיה זכאית, במקרה של הפרת איזו מהתחייבויותיי/נו על פי כתב התחייבות זה, לבקש מבית משפט מוסמך להוציא נגדי/נו צו מניעה זמני ו/או צווים אחרים במטרה למנוע ו/או להפסיק את ההפרה.
5. מבלי לגרוע מן האמור לעיל, אני/נו מתחייב/ים לפצות ולשפות את נתיבי איילון בגין כל נזק שייגרם לה או לחברות קשורות בה, לרבות הפסד ו/או פגיעה במוניטין כתוצאה מהפרת איזו מהתחייבויותיי/נו על פי כתב התחייבות זה, וזאת בנוסף לזכותה לנקוט כנגדי בצעדים משפטיים על פי כל דין. בנוסף, הנני/נו מתחייב/ים כי במידה ואפר/נפר הוראה מהוראות כתב התחייבות זה אשיב/נשיב לנתיבי איילון כל סכום שקיבלתי/נו, אם וככל שאקבל/נקבל, בגין ביצוע תפקידי/נו.
6. ידוע לי/נו כי המידע או חלקו מהווה מידע המוגן במסגרת חוק הגנת הפרטיות, תשמ"א - 1981, וכי הפרת איזו מההתחייבויות על פי כתב התחייבות זה עלולה להוות הפרה של הוראות החוק הנ"ל.
7. אם אדרש/נידרש מכוח חובה שבדין להציג את המידע בפני צד ג' כלשהו, אני/נו מתחייב/ים לטעון לחסיון, וכן מתחייב/ים להודיע לנתיבי איילון על קבלת דרישה כאמור, מיד עם קבלתה, על מנת שיהיה בידיה לטעון כנגד מסירת המידע.
8. ידוע לי/נו, כי התחייבויותיי/נו על פי כתב התחייבות זה אינן גורעות מתחולת כל דין והן בלתי הדירות ואינן מוגבלות בזמן, והן תעמודנה בתוקפן בכל עת ממועד חתימת כתב התחייבות זה ואילך, ובכלל זה אף לאחר סיום ביצוע תפקידי/נו, מכל סיבה שהיא.

מכרז למתן שירותי ניטור וניתוח אירועי אבטחת מידע וסייבר עבור חברת נתיבי איילון בע"מ

9. מבלי לגרוע מהאמור לעיל, ידוע לי/נו כי התחייבותי/נו כאמור בכתב התחייבות זה הנן מעיקרי ההתקשרות שביני/נו לבין נתיבי איילון, וכי במקרה של הפרת התחייבותי/נו לפי כתב התחייבות זה תחשב כהפרה יסודית של ההתקשרות שביני/נו לבין נתיבי איילון.
10. סמכות השיפוט ביחס לכתב התחייבות זה תהיה נתונה לבתי המשפט המוסמכים במחוז מרכז בלבד.

ולראייה באתי/באנו על החתום:

_____ תאריך:

_____ שם:

_____ ת.ז./ח.פ.

_____ חתימה: